MATH 314 Spring 2018 - Class Notes

2/21/18

Scribe: Tyler Schmitz

Summary: The use of Euler's Phi Function (Totient Function)

Notes:

$\phi(n)$ is equivalent to the number of residues mod n that are coprime to n
An example is $\phi(26) = 12$ (odd numbers and not 13).

If the number n is prime(p) then we take $\phi = p - 1$. For example $\phi(7) = 6$.

Product of 2 primes:

For $\phi(pq)$ where p and q are both primes, we use the Chinese Remainder Theorem
$x = (\_) \pmod{p}$
$x = (\_) \pmod{q}$

How many things can go into each equation?

p-1 and q-1 respectively

$\phi(pq) = (p-1)(q-1) = pq(1 - (1/p))(1 - (1/q))$

Example- $\phi(26) = \phi(2 * 13) = 26(1 - 1/13)(1 - 1/2) = 12$

The 12 coprime numbers are 1,3,5,7,9,11,15,17,19,21,23,25
And not 2,4,6,8,10,12,13,14,16,18,20,22,24,26

Π is used like Sigma for multiplication instead of addition.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

In this notation for every prime that divides n, there is another term added
A second example:

ex: $\phi(100) = 100\Pi(1 - 1/p)$
$\phi(100) = 100\Pi(1 - 1/p)$

The 2 prime factors of 100 are 2 and 5 so we have 2 terms. If there were more prime factors we would include these as well.

So:

$\phi(100) = 100\Pi(1-1/2)(1-1/5)$
$= 100(1/2)(4/5)$
$= 50(4/5)$
$= 40$

ex2: The prime factors of 429 are 3,11,13

$\phi(429) = 429\Pi(1-1/3)(1-1/11)(1-1/13)$
$= 429(2/3)(10/11)(12/13)$
$= 286(10/11)(12/13)$
$= 260(12/13)$
$= 240$
So there are 240 numbers coprime to 429

Euler's Theorem
If a and n are coprime then $a^{\phi(n)} = 1 \pmod{n}$. ex: Let $a = 3$ and $n = 4$.
$\phi(n) = \phi(4) = 4(1-(1/2)) = 2$.

Euler's Theorem says that $3^{\phi(4)} = 9 = 1 \pmod{4}$.

Note: that if $n = p$ is prime then Fermat's Little Theorem is a special case of Euler's Theorem.

The General Principle for modular arithmetic with exponents is if we work mod(n) then in the exponents we work mod Phi(n).

3-Pass Protocol

- Suppose Alice and Bob want to send package via UPS but Eve opens package through the email
- Alice and Bob have padlocks but they don't have the same keys
- Alice takes package and locks it with her key and sends it to Bob
- Bob locks it again with his padlock and sends it back to Alice

- Alice sends the box back to Bob after removing her lock
- Then Bob unlocks the box and reads the message because only his lock was still in the box

3-Pass Protocol Mathematically
We want to encode our message as a number m.

We need to pick a large prime number p, p isn't secret and Eve can know it.

Aice's key is a number coprime to (p - 1), call it "a", and Bob's key "b" is kept secret and is also coprime to (p-1).

Both are kept secret, Alice only knows hers and Bob only knows his.

Alice's Encryption Function is $E_A(m) = m^a \pmod p$.

Bob's Encryption function is $E_B(m) = m^b \pmod p$.

To decrypt Alice needs to undo raising something to the "a" power mod p.

Alice will compute $a^{-1} \pmod{p-1}$
Bob will compute $b^{-1} \pmod{p-1}$

Note: that if Alice encrypts m she gets $m^a \pmod p$

Now if she raises this to the $a^{-1} \pmod{p-1}$ then

$m^{a^{a^{-1}}} \pmod p = m^{aa^{-1}} = m^{k(p-1)^{-1}} \pmod p$
$= m^{(p-1)^k} \pmod p$

This is Fermat's Theorem.

The Whole process is:

- Alice's Encryption function is $E_A(m) = C_1 = m^a \pmod p$
- Sends C_1 to Bob
- Bob's Encryption function is $E_B(C_1) = C_2 = C_1^b \pmod p$
- Sends C2 to Alice
- Alice's Decryption function is $D_A(C_2) = C_3 = C_2^{a^{-1}} \pmod p$

- Bob's Decryption function is $D_B(C_3) = C_4 = C_3^{b^{-1}} \pmod{p}$